Dokobit
By Signicat

Authentication-based signature creation policy for Norwegian BankID Biometrics

This document is for public use.

Dokobit
By Signicat

Table of Contents

Dokobit
By Signicat

1. Policy Information

Name	Authentication-based signature creation policy for Norwegian BankID Biometrics
Document Number	DKB-SP-02282024 v1.0
Policy OID	1.3.6.1.4.1.54720.2.8.1
Policy Owner	Dokobit, UAB
Version	1.1
Publish date	2025-01-29

Dokobit
By Signicat

2. Revisions

Date	Specification version	Change
2024-02-28	1.0	Initial version
2025-01-29	1.1	Authentication method title update

Dokobit
By Signicat

3. Introduction

This signature policy defines requirements for authentication-based signatures using Norwegian “BankID Biometrics” as authentication mechanism. Authentication-based signatures are Advanced Electronic Signatures as per eIDAS regulation and are uniquely linked to signer by including required evidences to prove signing action by specified signer.

Dokobit
By Signicat

4. Terms And Acronyms

Term	Explanation
IdP	Identity provider.
Seal	This is the Trust Service Provider's signature on the signed document. It is commonly referred to as the *Seal*.
Signing ceremony	A sequence of activities like presenting the document, asking for the signers consent and the signing itself. The signing ceremony shall be conducted in a way that it afterwards is clear that the signer has willingly signed the document.
TSP	Trust Service Provider - the entity implementing this policy by packaging the signature.
Evidences	Collected evidences from Signing ceremony that are added as an additional metadata in PDF document.
PAdES	ETSI TS 103 172 V2.2.2 (2013-04) Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile.
RFC-3161	IETF RFC 3161: "Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP)".
eIDAS	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

Dokobit
By Signicat

5. Versioning And Backwards Compatibility

Signature policy version numbers consist of a major and a minor number, denoting major and minor versions.

A change of minor version is always backward compatible, and the new policy may be brought into effect without notifying relying parties.

A change of major version may introduce non-backward compatible changes.

Dokobit
By Signicat

6. About Signature Policies

The purpose of a signature policy is to specify requirements for the signing process including requirements for signature creation and verification process.

The primary users of this policy will be users using authentication-based signatures (relying parties). The policy will help relying parties to better understand the information contained in an authentication-based signature, and on what basis it can be trusted and used.

Dokobit
By Signicat

7. Scope And Structure

This signature policy defines requirements for creating and validating signature based on an arbitrary method of signer authentication.

The normative parts of the policy are:

General process requirement defines high-level requirements for the overall signing process.

1. **Signature creation requirements** defines requirements for the format used for the signature
2. **Validation requirements** defines the validation of authentication-based signature.

8. Signature Creation Requirements

Authentication-based signatures work in the following way:

1. A Trust Service Provider (TSP) arranges a signing ceremony: It presents the documents to be signed and collects the user's explicit consent/intention to sign the documents.
2. The user authenticates using Norwegian "BankID Biometrics". The TSP collects authentication proof.
3. The TSP collects traces and context in audit logs.
4. The TSP adds collected evidence as a metadata in XML format to the original PDF document.
5. The TSP seals a PDF document with collected Evidences using TSP's Advanced Electronic Seal with Qualified Certificate.
6. The sealed PDF results as a document with user's signature.

8.1 Evidence Structure

The following information must be collected from Signing Ceremony:

Element/Attribute	Description	Example	Required
Global			
SigningIdentifier	Unique signature identifier in Dokobit system	5e00fb8febc7d2532fce637ca56079baaddc6780	true
SigningTime	Signing time in ISO 8601 full date and time format	2022-01-14T11:23:27+02:00	true
PolicyId	Policy ID that was used for creating the signature	1.3.6.1.4.1.54720.2.1.1	true
LiabilityTier	Liability tier for created signature	1	true
Client Environment			

UserAgent	User agent string representing client environment	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/ 537.36 (KHTML, like Gecko) Chrome/ 97.0.4692.71 Safari/537.36	true
Ip	Signer IP address	127.0.0.1	true
Server Environment			
Dns	Server DNS address	app.dokobit.com	true
VersionIdentifier	Codebase version identifier	202201131550-d14c26a5e210a227e24ae2f10d062653bc336fc3	true
Signer Details			
Firstname	Signer firstname detected using authentication mechanism	Firstname	true
Lastname	Signer lastname detected using authentication mechanism	Lastname	true
Identifier	Unique signer identifier specifying code type, issuing country and code	PNONO-30101010101	true
Code	Signer code representing unique person in authentication mechanism scope	30101010101	true
CountryCode	Country code specifying in which country code was issued	no	true
BirthDate	Signer birthdate	1990-01-14	false

User Actions			
Name	Action made by user. Possible values: user-authentication, document-view, document-sign	user-authentication	true
TimeStamp	Action time in ISO 8601 full date and time format	2022-01-14T11:23:27+02:00	true
User Action Details			
Method	Method used for authentication. Possible values: bankid_no.	bankid_no	Required only for action “user-authentication“
TransactionId	Transaction identifier in authentication system	7f22fd6a-3d46-4d5a-ae56-6de3c53e1873	Required only for action “user-authentication“

Dokobit
By Signicat

Example of evidence structure:

```
<?xml version="1.0" encoding="utf-8"?>
<DokobitAuthenticationBasedSignature xmlns="https://dokobit.com/authentication-based-
signatures" Version="1">
  <SigningIdentifier>5e00fb8febc7d2532fce637ca56079baaddc6780</SigningIdentifier>
  <SigningTime>2022-01-14T11:23:27+02:00</SigningTime>
  <PolicyId>1.3.6.1.4.1.54720.2.1</PolicyId>
  <LiabilityTier>1</LiabilityTier>
  <Environment>
    <Client>
      <UserAgent>Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36</UserAgent>
      <Ip>127.0.0.1</Ip>
    </Client>
    <Server>
      <Dns>app.dokobit.com</Dns>
      <VersionIdentifier>202201131550-d14c26a5e210a227e24ae2f10d062653bc336fc3</
VersionIdentifier>
    </Server>
  </Environment>
  <SignerDetails>
    <Firstname>Firstname</Firstname>
    <Lastname>Lastname</Lastname>
    <Identifier>PNONO-30101010101</Identifier>
    <Code>30101010101</Code>
    <CountryCode>no</CountryCode>
    <BirthDate>1990-01-14</BirthDate>
  </SignerDetails>
  <UserActions>
    <UserAction>
      <Name>user-authentication</Name>
      <TimeStamp>2022-01-14T11:23:27+02:00</TimeStamp>
      <Data>
        <Method>bankid_no</Method>
        <TransactionId>7f22fd6a-3d46-4d5a-ae56-6de3c53e1873</TransactionId>
      </Data>
    </UserAction>
    <UserAction>
      <Name>document-view</Name>
      <TimeStamp>2022-01-14T11:23:27+02:00</TimeStamp>
    </UserAction>
    <UserAction>
      <Name>document-sign</Name>
      <TimeStamp>2022-01-14T11:23:27+02:00</TimeStamp>
    </UserAction>
  </UserActions>
</DokobitAuthenticationBasedSignature>
```

Dokobit
By Signicat

9. Signature Validation Requirements

Authenticaton-based signatures should be validated in the following way:

1. If a valid seal with any certificate that is specified in Appendix A is found in document, validation of authentication-based signature should continue, otherwise signature does not meet requirements of this policy.
2. Seal dictionary contains “Metadata” element which refers to Collected Evidences in PDF document.
3. Information that resides in Collected Evidences should be treated as a trusted information.

Dokobit
By Signicat

10. Limitation Of Liability

TSP assumes the liability only for the execution of the Signing ceremony and provides the services with two different limitations:

- Tier 1 (Basic Liability). This tier is for the documents that don’t exceed the value of EUR 100 as Dokobit will be liable up to EUR 100 per signed document.
- Tier 2 (Advanced Liability). This tier is for the documents that don’t exceed the value of EUR 10 000 as Dokobit will be liable up to EUR 10 000 per signed document.

11. Appendix A (Normative): Certificates Used For E-Sealing PDF Documents

The following certificates are used as a trust anchor for creation and validation of authentication-based signatures using Norwegian “BankID Biometrics“.

1. “Norwegian BankID Signature by Dokobit” Qualified Certificate for Seal is issued by Qualified Trust Service Provider - SK ID Solutions - in accordance with SK ID Solutions Certification Practice Statement for KLASS3-SK - SK-CPS-KLASS3-v8.0 which is available at *https://www.sk.ee/upload/files/SK-CPS-KLASS3-EN-v8_0_20190815.pdf*.

Certificate details:

Key	Value
Serial number	57 BC 42 76 D3 79 E4 45 6F 32 08 7F 46 14 8D 02
Valid from	2024-02-28T10:28:58Z
Valid to	2027-03-29T11:58:57Z
Subject information	
Organization identifier	NTRLT-301549834
Serial number	301549834
Location	Vilnius
Country	LT
Organization	Dokobit, UAB
Common name	Norwegian BankID Signature by Dokobit
Issuer information	

Key	Value
Organization identifier	NTREE-10747013
Organizational unit	Sertifitseerimisteenused
Organization	AS Sertifitseerimiskeskus
Country	EE
Common name	KLASS3-SK 2016

11.1 Certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIGbjCCBFagAwIBAgIQV7xCdtN55EVvMgh/RhSNAjANBgkqhkiG9w0BAQsFADCB
hjELMAkGA1UEBhMCRUUxIjAgBgNVBAoMGUFTIFNlcnRpZml0c2VlcmltaXNrZXNr
dXMxITAfBgNVBAsMGFNlcnRpZml0c2VlcmltaXN0ZWVudXNlZDEXMBUGA1UEYQwO
TlRSRUUtMTA3NDcwMTMxFzAVBgNVBAMMDktMQVNTMy1TSyAyMDE2MB4XDTI0MDIy
ODEwNTg1OFoXDTI3MDMyOTEwNTg1N1owgaYxLjAsBgNVBAMMJU5vcndlZ2lhbiBC
YW5rSUQgU2lnbmF0dXJlIGJ5IERva29iaXQxEjAQBgNVBAUTCTMwMTU0OTgzNDEY
MBYGA1UEYQwPTlRSTFQtMzAxNTQ5ODM0MRUwEwYDVQQKDAxEb2tvYml0LCBVQUIx
EDAOBgNVBAcMB1ZpbG5pdXMxEDAOBgNVBAgMB1ZpbG5pdXMxCzAJBgNVBAYTAkxU
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAkRKxKp0TReYTfLy2kZEz
2O4iE4RtC880bUDtkuBmtxy6kydaoImmlYz5deYm2rAHdbWU4krnku+2uMfY6HzW
XecdQt5b4fG++wIkaPdcrN2OqAlSC/Fw35pYd4BNX7kUSVDt7WMR0h+wtjL6s41c
NUhXxKR6d4uXHy6iHMboljIW1auoOxUb+qhPGwvZ4e8nR1jbVjXQ/1SZigVcnvrO
Mh+2dCaO10xjcuhQkb2+mAEP2dr1lvd/OPdBh6LL8KQUdnfCubQuj2mj1P8XK4N3
7k7gXXBFA886fxPJMVnJo3Bmrg/oGbNcqRYlNeckZ1LwPy3E0mCaWNhwJzxdxCRY
WwIDAQAFo4IBtDCCAbAwCQYDVR0TBAIwADAfBgNVHSMEGDAWgBSuXlj18vLZwY7Z
704H23XKUOKHADB7BggrBgEFBQcBAQRvMG0wQQYIKwYBBQUHMAKGNWh0dHBzOi8v
Yy5zay5lZS9LTEFTUzMtU0tfMjAxNl9FRUNDUkNBX1NIQTM4NC5kZXIuY3J0MCgG
CCsGAQUFBzABhhxodHRwOi8vYWlhLnNrLmVlL2tsYXNzMy0yMDE2MFMGA1UdIARM
MEowMAYJKwYBBAHOHwcDMCMwIQYIKwYBBQUHAgEWFWh0dHBzOi8vd3d3LnNrLmVl
L2NwczAJBgcEAIvsQAEBMAsGCSsGAQQBzh8JATCBgAYIKwYBBQUHAQMEdDByMAgG
BgQAjkYBATATBgYEAI5GAQYwCQYHBACORgEGAjBRBgYEAI5GAQUwRzBFFj9odHRw
czovL3NrLmVlL2VuL3JlcG9zaXRvcnkvY29uZGl0aW9ucy1mb3ItdXNlLW9mLWNl
cnRpZmljYXRlcy8TAmVuMB0GA1UdDgQWBBQ6aAtGfdVjyEmCCQ9CggFwTtdQTTAO
BgNVHQ8BAf8EBAMCBkAwDQYJKoZIhvcNAQELBQADggIBAE7tWFGARmNIeltJjPpl
ULHGZ5EvsXNHzbrC0FV9QTT56pVrjdEH4n+8XxrjaWAHHvpRVbHV+dpUiNJzbFBY
hro+lgtECIG7tc0sixUZx5jQJWDL2yHJxtVTL5JArfTGwi2P4PKw76yceE6QHtUL
bTzlZEPjW0/JGlfqKR9cc6vD7BrldbJxkN79k4pkKo61KhEDz2/2S41i7ZmTKbe6
Q6JDMdLggyHcK19clrZ1k/jQkjXWEs6fXxXluBljGsXXCPzoetZnWAmGmhkv4Pur
lhIpAB1iUcVe5H2mmvRWcGDq4xlOsB8CiwhPLFWQ53x92Ahn6DwM38ADVRH3h/UL
nwjLiPH070fzGSEbKci0bJkDSEfKFLMP5O6AX/KDSNDpM6MKyerMdiPeF/g69u9T
m5aFt9GOslvMGGtmrZ3W2jrUK9y5p6Bb8k7cxO7pfSIVkXJjJEb9HiJ4xW15ickg
pNJfGEl9FGgS9w3Gmu8SgjiVutLYM7DIzcrohS1sM3nTTfzdJwfbDMkvEnQSNVth
Ax6wNOltlmhCBBjdgPW9FYkj+ZJNK4e/vtnWB+/prUJnkTHqz/P+8PB6caOJVC2s
kwJRAtZqMElwNyH4yvcsUNNF3erXlZ9+8HSzrh1Bta6y8EEiBx46sQKHqSHfhfUR
IP/El3XTWwUuFVUIW5bMoye0
-----END CERTIFICATE-----
```